Security threats in cloud computing

Article · July 2015

DOI: 10.1109/CCAA.2015.7148463

CITATIONS
6

READS
1,033

3 authors, including:

Neha Kajal
The Northcap University
2 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Prachi Chaudhary
The Northcap University
39 PUBLICATIONS **95** CITATIONS
SEE PROFILE

CLOUD COMPUTING SECURITY:

AMAZON WEB SERVICE

Saakshi Narula
M.tech Student
Department of CSE & IT
ITM University
Gurgaon ,India
saakshinarula@yahoo.in

Arushi Jain
M.tech Student
Department of CSE & IT
ITM University
Gurgaon ,India
arushijain_1992@yahoo.com

Ms. Prachi
Associate Professor
Department of CSE & IT
ITM University
Gurgaon ,India
prachi@itmindia.edu

***Abstract*—Cloud Computing is a recently emerged model which is becoming popular among almost all enterprises. It involves the concept of on demand services which means using the cloud resources on demand and we can scale the resources as per demand. Cloud computing undoubtedly provides unending benefits and is a cost effective model. The major concern in this model is Security in cloud. This is the reason of many enterprises of not preferring the cloud computing. This paper provides the review of security research in the field of cloud security. After security research we have presented the working of AWS (Amazon Web Service) cloud computing.AWS is the most trusted provider of cloud computing which not only provides the excellent cloud security but also provides excellent cloud services. The main aim of this paper is to make cloud computing security as a core operation and not an add on operation.**

Keywords— Cloud Computing, Trusted Computing, Information Centric Security, Amazon Web Service.

I. INTRODUCTION

The word "cloud" was used by Google's CEO Eric Schmidt to describe the business model of providing services across the internet in 2006. To state various ideas the term cloud was used as marketing term [1]. Classification of clouds is done as public, private and hybrid. Services of three types are offered by cloud providers are Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) [2]. Cloud computing has a focus on maximizing effectiveness of the shared assets. Cloud computing have certain features like they are agile, have reduced cost, easier maintenance, reliable, secure, scalable, etc. Cloud computing involves communication over a loose coupling mechanism which involves multiple cloud components. Certain security issues faced by cloud computing include sensitive data access, data segregation, privacy, authentication, bug exploitation, recovery, accountability, account control [3][23].

A. What is Cloud Computing?

It is one of the approaching IT industry murmured words- the users move their applications and data to the remote cloud so that they can have a simple and pervasive way of accessing.
Clouds are categorized in two ways:
a) On the basis of location of cloud computing.
b) On the basis of type of services offered.

B. On the basis of location of the cloud

These are further categorized as:
a) Private Cloud: These are allocated to a particular organization and are not divided among any specific firm. Private clouds have higher cost and security in comparison to public clouds. Further types of private clouds are private clouds and externally hosted private clouds.
b) Public Cloud: In public cloud, at the vendor's premises the computing infrastructure is hosted by the traders of the cloud. The user has no clarity and control hosted by the computing framework. The computing foundation is shared between with some companies.
c) Hybrid Cloud: This type of clouds is cost-effective and scalable. When we combine the use of public and private clouds together it is called as hybrid cloud. This aims in minimizing change.

C. On the basis of service provided

These are categorized in the following ways:
a) Infrastructure as a Service (IaaS): Using the principles of cloud computing, services related to hardware are offered. These include storage services or virtual servers.
b) Platform as a Service (PaaS): Development platform on the cloud is offered by them. Distinct vendors provide platform that are not consistent.
c) Software as a Service (SaaS): Complete software services are offered on the cloud. Software

2327-0659/15 $31.00 © 2015 IEEE
DOI 10.1109/ACCT.2015.20

application can be accessed by the users hosted by the cloud vendor on the basis of paying as per use. The nomenclature of cloud computing consists of a part which is known as Software as a favor. [24].

II. SECURITY IN CLOUD COMPUTING

Cloud computing undoubtedly provides very good service to the user but still many organizations do not support cloud computing because of the security issues. The main security issues are data security and privacy protection. These security issues hinders the managers or customer to support the services provided by cloud computing [6].This is the reason why cloud computing not gaining the expected market size. Cloud security is the responsibility of both the cloud provider and cloud consumer. There should be the relationship of trust between them before availing any cloud service.[7]. It is the responsibility of management to take care of security risk so as to protect data. There are many risks associated with the cloud computing .Some of them are: Security, service providers, Management and Control, Laws and regulation, virtualization risks, lack of standards and auditing, uncontrolled viable cost etc. The risk which is of most concern is Security [5]. Cloud computing is the just the virtual environment for the customer who are using the cloud services in which he will give its data to the cloud without knowing even the location of the data. The data can be there with thousands of other data on the cloud. So the most important facilities that storage provider should provide is Confidentiality, Integrity and Availability (CIA)[9].A model should be developed that promotes CIA.CIA can be provided by –encrypting the data, access control to prevent unauthorized user to access data and scheduled back up should be there to ensure availability.

III. SECURITY RESEARCH

In order to tackle the security issues in cloud there is a need of some research in this area so as to provide security in the cloud computing and attracting more number of users so as to save the resources and time.

The models of security research are:

a) Trusted computing
b) Information Centric Security [ICS].

A. Trusted Computing [TC]:

The main reason for the IT companies not using the cloud is lack of trust on the service provider in cloud computing. To gain that trust the service provider also have to work hard by providing better security policies. This mutual trust can be generated by involvement of third party who attest both the customers and cloud provider and this is known as remote server attestation [4,1].TC system was considered to be very important because data security is considered to be the core operation and not the add-on operation. TC system encrypts the data and application and gives the decryption key to the trusted program and information [13]. Nowadays manufacturers provide the TC services in the computers by adding some new hardware to the computers.

Trust Computing Platform[TCP]:-The two services provided by TCP are authenticated boot and encryption. The TCP has two components: Trusted virtual machine monitors [TVMM] and trusted coordinator. TVMM hosts the customer's virtual machines [VMs] and also give protection against inspection and modification of customer's VM. Trusted coordinator is responsible for running customer's VM securely by some set of nodes. These nodes should be within security perimeter and should run the TVMM then only these nodes are said to be trusted node [14].

B. Information Centric Security [ICS]:

It refers to security of information rather than security of networks or applications. One way to provide ICS is encrypting the information. The owner, who has the decrypting key can only control the access of the data and no one else can read or write the information. But strong encryption may not be useful because in the cloud the data is processed in the unencrypted form[4].ICS architecture is made of 4 services arranged horizontally and not vertically. The 4 services are [15].

a) Storage infrastructure services
b) Data services
c) Management services
d) Access services

The architecture of Information centric security protects the information by monitoring and enforcing the policies of security or privacy. The individuals who are dispersed all over can now share their documents securely. The documents now contain security rules with them so that whenever there are logs capture activities then the security policies are enforced. The officers or manager of privacy or security policies are responsible for making the usage policies and the policy management engine is used to enforce the security rules over the documents or secret documents.ICS architecture is responsible for controlling, monitoring and enforcing the security over the confidential documents [16][15].

1. Access Service	a. Authentication b. Authorization
2. Management Service	a. Key Management b. Policy Management c. Monitoring d. Reporting
3. Data Service	a. Discovery b. Classification c. Data Modeling d. Data Mapping e. Meta data repository
4. Storage Infrastructure Service	a. Secure Storage Network b. Secure Storage Partitioning c. Cryptographic Processing d. ILM Services e. Infrastructure services

Fig. 1

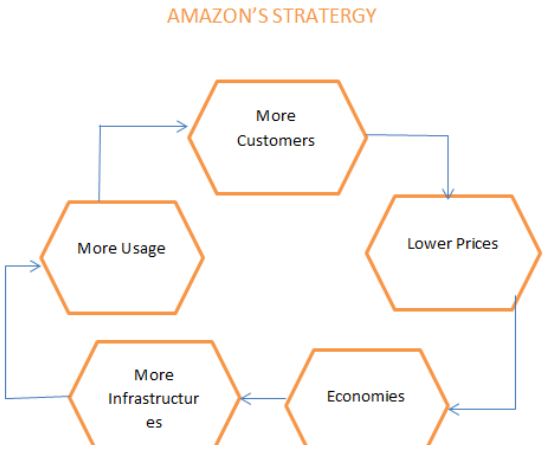

Fig. 2

IV. AWS (AMAZON WEB SERVICE)

AWS is the cloud computing provider. This service is a perfect example of true cloud computing which not only provides excellent cloud services but also provides confidentiality; integrity and availability of the customer's data [9].AWS give the on demand services. The IT resources are available at cheap prices and no upfront investment is required for the resources. The customer just has to pay for the resources that he consumes on variable basis. AWS provide the flexibility in terms of amount of resources the customers need. If they need more than demanded then they can easily scale up and if they don't need the resources that they have then they can turn them off and stop paying. Another benefit of AWS is it makes the work easier and faster. With traditional architecture it was difficult to develop the application as it takes lot of time to get a server. But with AWS cloud computing one can deploy hundreds or thousands of servers without any delay. Hence AWS allows quick development and deployment of an application and hence it allows the team to experiment more frequently.

AWS not only provide resources to develop an application but also helps in deploying the application globally at minimum cost. Traditionally it was difficult for a company to provide performance to the distributed users so they concentrate on only single geographical region at a time. But with the help of AWS this problem was solved and now one can deploy its application all around the world and provide better experience for customers.[20]

AWS provides wide range of cloud computing services that helps in development of a sophisticated application.

V. AWS SECURITY PROCESS

For AWS, Confidentiality, Integrity, and Availability (CIA) [9,17] of the user's data is most important task. The aim of AWS is to maintain the customer confidence and trust.

A. AWS infrastructure

AWS infrastructures made or designed on the basis of the security practices that are very important to secure the customer's data. AWS infrastructure contains hardware, operational software, security standards, network and other important facilities. AWS data centers have a very innovative architecture because of their huge experience in designing and constructing data centers. High level security is there during the physical access of AWS data centers. Professional security staff is hired for data security. They use electronic equipment like video surveillance, CCTV cameras, intrusion detections system etc. Visitors or contractors have to present their identification which is signed by authorized staff and are allowed to access if they have business needs. The environment of the data centers is controlled

a) Automatic fire detection and suppression equipment to reduce risk.

b) 24*7 Uninterrupted Power Supply.

c) Climate control is there in order to maintain the temperature for working of servers and other hardware.

d) All equipment is managed, so if any issue is raised then it should be immediately identified.

B. Network Security:

AWS has an outstanding network security as it has an outstanding network architecture which is properly controlled and managed. Following are the

reasons for the world class network architecture of AWS:

a) Secure Network Architecture
b) Secure Access Points
c) Transmission Protection
d) Amazon Corporate Segregation
e) Fault Tolerant Design
f) Network monitoring and Protection

Secure Network Architecture is attained by the network devices such as firewall which manages and controls the boundary of network. Traffic flow policies, access control list (ACL), is generated to control the flow of informational is approved by Amazon Information Security. Secure Access Point indicates that AWS has limited number of access points so as to perform proper monitoring of communication. The access points of customers are called API endpoints. These access points help in access of secure HTTP (HTTPS).Transmission Protection:-One can make connection to the AWS access point via HTTS using SSL (Secure Socket Layer) protocol. This protocol provides many security services like protection against message forgery, tampering etc. Next is Amazon corporate segregation which means segregation of Amazon Production network from Amazon Corporate network by the network devices. The developer or manager cannot directly access the network devices even for maintenance. They need to access through AWS ticketing system. Once the personnel is approved they can then access the AWS network with help of bastion host. Fault Tolerant Design:-AWS has designed its architecture in such a way that if any hardware or software failure then it should have minimum impact on the customer.AWS has provision of storing data with multiple geographical regions with each region having independent failure zone.

Network monitoring and protection:-AWS has a world class monitoring and control system as it has automated monitoring system which automatically detects the defects; any unauthorized access or any unusual activity. Some instruments are there which help in monitoring. For e.g. Alarms are set to notify any unusual activity.

VI. RELATED RESEARCH WORK

The concept of Cloud computing was initiated in 1950s. The providers of cloud computing at a low expense can build datacenters because of experts in organizing and computational resources which are provisional. Cloud computing allows for efficient computing. In Cloud Computing, there are different existing technologies that bind together to run business in efficient and different way [1]. Being a user we do not require being experts for controlling the cloud infrastructure [2]. Many small and large companies are involved in cloud computing like Microsoft, IBM, Facebook, Yahoo, Google, Oracle and many more. Cloud Computing has some advantages like flexibility, capital investment, portability, scalability and some disadvantages as well like security, dependability, little or no reference etc. Some of the challenging research issues of cloud computing which include Cloud data management and security, Data Encryption, Interoperability, access control, Migration of virtual machines, Platform management, Service Level Agreements [2]. Cloud Computing was not a new idea, it was envisioned in 1960s by John McCarthy with the idea of providing it to the general public for profit and usefulness. The word “Cloud” in 1990s was used to represent large networks like the ATM network .Virtual Private Network (VPN) services were provided by telecommunication services with better quality and lower cost. Cloud Computing uses concepts and best practices which are already established, so it is an old concept. We maintain applications and data using remote servers and internet in Cloud Computing technology.. In 2009, Pearson described privacy issues in cloud computing. Enisa presented cloud security risk assessment in 2009 [21]. Amazon released Amazon Web Services (AWS) that is based on Server Virtualization Technology in 2006-2007 [22]. Open-source cloud-software which was known as OpenStack was launched jointly by Rackspace Hosting and NASA in July 2010. IBM SmartCloud framework was announced by IBM for supporting Smarter Planet on 1st March 2011. Oracle announced Oracle Cloud on 7th June 2012. Detailed analysis and description was given on each security issue and investigation was done from cloud computing service delivery models [6]. SOA and Virtualization are used technologies through which some security issues arise and the major cloud security problem is isolation and multi-tenacy [10]. For maximizing resource utilization, cloud computing helps in storing data at remote site which results in critical data protection [11]. Security architecture system is proposed to overcome the various security issues raised [15]. Services like AWS are available only when we demand and we pay for what we use which is an important advantage for disaster recovery [19].

VII. CONCLUSION

Cloud Computing undoubtedly provides many services and has uncounted advantages but still there are many problems that still exits and need to be solved to increase the market of such a world class technology [19].The concern in the cloud computing is SECURITY around data, access and privacy protection. Cloud computing should be secure and

robust and should mitigate the risks. According to the analysis of cloud computing it was found that security should be the core operation rather than an add on operation. AWS(Amazon Web Service) has an outstanding performance in cloud computing because of the its excellent work in the area of Security of data. Some of work of the AWS is

a) Providing network security
b) Build real time sliding window dashboard over streaming data
c) AWS for Disaster Recovery (DR).[18]
d) Security at scale: logging in AWS.
e) Securing data with encryption
f) Backup and Recovery approach

These security services provided by AWS are the reason that customers have faith in its services. So building trust by providing security services should be the main aim of cloud computing.

REFERENCES

[1]] Qi Zhang, Lu Cheng, RaoufBoutaba. Cloud Computing: State-of-the-art and research challenges. J Internet ServAppl (2010).

[2] Rabi Prasad Padhy, ManasRanjanPatra, Suresh Chandra Satyapathy. Cloud Computing: Security Issues and Research Challenges. IJCSITS Vol. 1, No. 2, December 2011.

[3] Meiko Jensen, JorgSehwenk et al. "On Technical Security Issues in Cloud Computing". IEEE International Conference on Cloud Computing, pp 109-116, October 2009.

[4] Shubhashis Sengupta, Vikrant Kaulgud, Vibhu Saujanya Sharma. Cloud Computing Security-Trends and Research Directions. 2011 IEEE World Congree on Services.

[5] Mariana Carroll, Alta van der Merwe, Paula Kotze. Secure Cloud Computing. Benefits, Risks and Controls. 2011 IEEE.

[6] Deyan Chen, Hong Zhao. Data Security and Privacy Protection Issues in Cloud Computing. 2012 International Conference on Computer Science and Electronics Engineering. 2012 IEEE.

[7] Akhil Behl, Kanika Behl. An analysis of Cloud Computing Security Issues. 2012 IEEE

[8] Amreen Khan and KamalKant Ahirwar. Mobile Cloud Computing as a Future of Mobile Multimedia Database. IJCSC, Vol. 2,No. 1, January-June 2011, pp. 219-221.

[9] John Harauz, Lori M. Kaufman, Bruce Potter. Data Security in the World of Cloud Computing. IEEE July/August 2009.

[10] Al Morsy. M. Grundy, J & Mueller, I. (2010). An analysis of the cloud computing security problem. 17th APSEC 2010. 30 November-03 December 2010.

[11] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham. Security Issues for Cloud Computing. Technical Report. February 2010.

[12] Shipra Shukla, Rakesh Kumar Singh. Security of Cloud Computing System using Object Oriented Technique. 26th-28th July,2012 IEEE.

[13] Zhidong shen, Qiang Tong. The Security of Cloud Computing System enables by Trusted Computing Technology.2nd ICSPS 2010 IEEE.

[14] Nuno Santos, Krishna P. Gummadi, Rodrigo Rodrigues. Towards Trusted Cloud Computing.

[15] Dayanand Sagar Kukkala, V.P. Krishna Anne, Rajasekhara Rao Kurra. Data Security in Cloud: A proposal Towards the Security Isuues. IJCSET. December 2011. Vol 1, Issue 11, 731-736.

[16] Jon Oltsik. The Information-Centric Security Architecture. White Paper.

[17] Amazon Web Services: Overview of Security Processes. June 2014 White Papers.

[18] Glen Robinson, Attila Narin, and Chris Elleman. Amazon Web Services- Using AWS for Disaster Recovery. October 2014 White Papers.

[19] Deyan Chen, Hong Zhao. Data Security and Privacy Protection Issues in Cloud Computing. 2012 Internationals Conference on Computer Science and Electronics Engineering.

[20] http://aws.amazon.com/what-is-aws/

[21] Flavio Lombardi, Roberto Di Pierto. Journal of Network and Computer Applications. Journal of Network and Computer Applications.

[22] Ling Qian, Zhiguo Luo, Yujian Du, and Leitao Guo. Cloud Computing: An Overview.

[23] Mladen A. Vouk, "Cloud Computing- Issues, Research and Implementations" Journal of Computing and Information Technology –CIT 16, 4, pp 235-246, 2008.

[24] SumitKhurana, Anmol Gaurav Verma. Comparison of Cloud Computing Service Models: SaaS, PaaS, IaaS. IJECT Vol. 4. April-June 2013.